HOW TO: Proof of Concept
One-Arm (Sniffer) Mode
FortiOS 5.2

Fortinet LATAM SE Team

Version 2.1

September 2014

DOCUMENT CHANGES LOG

Version	Author	Date	Change(s)
1.0	Marcelo Mayorga	Sep 5, 2013	Main document template, FortiGate configuration
1.1	Marcelo Mayorga	Sep 9, 2013	Changed template, FortiAnalyzer configuration
1.2	Marcelo Mayorga	Sep 22, 2013	Report Generation
	Vadin Corrales		Fixed errors and added comments
1.3	Marcelo Mayorga	Nov 7, 2013	Added reference
	Vadin Corrales		Fixed errors and added comments
1.4	Marcelo Mayorga	Dec 11, 2013	Updated document to FortiAnalyzer 5.0.5
	José Luis Laguna Merino		Added check-list section
	Matteo Arrigoni		Content fixes
1.5	Marcelo Mayorga	Dec 13, 2013	Changed on report generation section, Added customer report import “Application and Risk Analysis – One Arm”
	Martin Hoz		Added disclaimer and some content correction
1.6	Marcelo Mayorga	Dec 18, 2013	Fixed minor changes
	Martin Hoz		Fixed errors, added content on disclaimer, benefits and drawbacks and others
1.7	Marcelo Mayorga	Dec 21, 2013	Changed IPS configuration (enable all signatures)
			Updated document for FortiOS 5.0.5
			Simplified ARA One Arm datasets conf
			Added sample report
1.8	José Luis Laguna Merino	Apr 17, 2014	Added FortiAnalyzer best practice regarding disk quota.
1.9	Michel Barbosa	May 15, 2014	Added presentations tips and minor changes Created Quick Configuration Script
2.0	Marcelo Mayorga	Sep 1, 2014	Modified the document for FortiOS 5.2 and FortiAnalyzer 5.2 Changed document template Fixed minor details Added Quick Configuration Script as part of the document
2.1	Marcelo Mayorga	Sep 4, 2014	Added Directory integration for user identification

CONTACT

For comments or suggestions about this document, please contact document coordinator Marcelo Mayorga (mmayorga@fortinet.com)

DISCLAIMER

This documents is intended for Fortinet engineers with experience on information security, networking and at least one year configuring FortiGate and FortiAnalyzer.

This document is NOT intended for end users or people not used to install and/or operate network security technology.

Fortinet, its employees and affiliates are not responsible for any service affection or impact that could be generated while doing any activity described in this document.

INTRODUCTION

DOCUMENT GOAL

The goal of this document is to provide a guideline on how to do a Proof of Concept (POC) and show how a network might be protected, without the necessity of building a complete working vehicle for that purpose. This is achieved by means of FortiGate capability of acting as a one-arm device in the network.

PREPARE YOURSELF

Similar to what happens in an actual product deployment, the success of a Proof of Concept is extremely tied to a proper and responsible planning. Before doing any action, make sure you:

1. Call the customer, gather and set expectations.
2. Gather and document information, credentials, IP address schemes, etc.
3. Products are registered and have a valid contract (See: “Registering your unit” below).
4. Make sure paperwork and administrative tasks have been done. Remember some companies require approval in order to allow gear to get into their premises or be installed it into their network.
5. Last but not least, make sure you know the entire process. Try the whole procedure at least once on a controlled environment (may be your own company network). The last thing you want to do is to look doubtful in front of a potential customer.

SNIFFER MODE/ONE-ARM/SPAN MODE – BENEFITS AND DRAWBACKS

Before getting into the technical stuff is important to understand that deploying a FortiGate in a one-arm topology has benefits and drawbacks.

NOTE

On this document the terms *sniffer*, *one-arm* and *span* modes are used interchangeably

Benefits:

- Non-intrusive: Does not require mayor changes nor will affect network performance.
- Provides real-time visibility of customer's traffic
- Allows a customer (prospect) to familiarize with Fortinet's GUI without the associated risk of interfering with production traffic.

Drawbacks:

- Not valid for sizing or performance measurement: Processing traffic in sniffer mode does not demand the same kind and amount of resources as it takes doing inline inspection.
- It does not provide (and shouldn't be positioned as) security protection. The focus is on visibility
- Some traffic might not be caught and some FortiGate inspection features won't work on this mode.
- SSL Inspection is not supported in sniffer mode.

REQUIRED GEAR AND VERSIONS USED

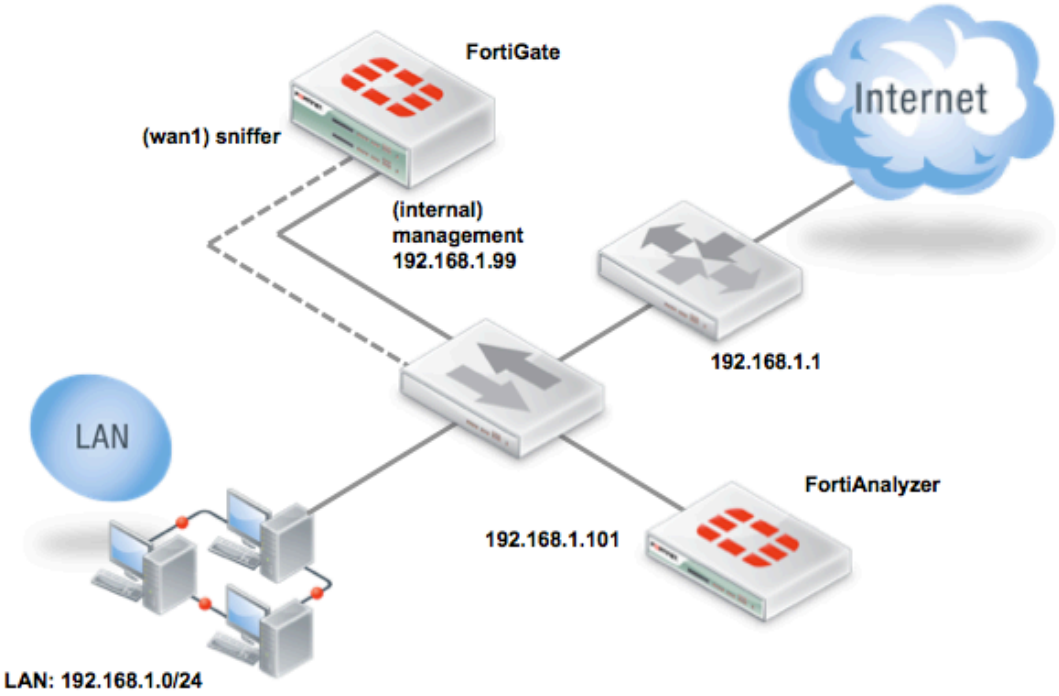
For this document, the following versions were used.

- FortiGate: This document was created using FortiOS 5.2 (build0610).
- FortiAnalyzer: This document was created using FortiOS 5.2 (build0618).

While the hardware models used on this document are a FortiGate-60C and a FortiAnalyzer-VM, It is recommended to properly size the right hardware. If in

doubt, size like if the FortiGate were going to do full inline inspection and the FortiAnalyzer were to receive full logging.

NETWORK TOPOLOGY



REGISTERING YOUR UNIT

Remember that your FortiGate unit must be registered within Fortinet Support system in order to be able to access FortiGuard services and thus updating its security databases (AV, IPS, Applications, etc.).

For a detailed guide on how to register a Fortinet product, read the following document: https://support.fortinet.com/Download/RegistrationGuide.pdf

TYPOGRAPHIC CONVENTIONS

Whenever you see this

```
CLI
```

It means the following steps can be done using the Command Line Interface

Whenever you see this

```
GUI
```

It means the following steps can be done using the Graphical User Interface

HANDS-ON: FORTIGATE CONFIGURATION

This document has been created starting from a factory default configuration. If you're not an experienced user we recommend you to restore your FortiGate to defaults before moving on. Make sure you backup your configuration before moving forward.

1. Connect to your FortiGate either through CLI (SSH/Telnet/Console/FortiExplorer) or using the embedded CLI Console widget in FortiGate's GUI
2. Execute:

CLI

```
# exec factoryreset
This operation will reset the system to factory default!
Do you want to continue? (y/n)y
```

DISABLE DHCP SERVER

If you're starting from a factory configuration is probable that you have a DHCP server configured. Make sure you delete it in order to avoid any conflict with other DHCP servers in the network.

CLI

```
# config system dhcp server

(server) # show
config system dhcp server
    edit 1
        set default-gateway 192.168.1.99
        set dns-service default
        set interface "internal"
            config ip-range
                edit 1
                    set end-ip 192.168.1.254
                    set start-ip 192.168.1.100
```

```
                next
            end
        set netmask 255.255.255.0
    next
end


(server) # purge
This operation will clear all table!
Do you want to continue? (y/n)y
```

Repeat “delete” operation for any entry listed.

CONFIGURING MANAGEMENT INTERFACES

With default configuration, login to the FortiGate and configure one interface to be used for management purpose.

NOTE

Default management interface will depend on FortiGate model. If you don’t know which interface to use, take a look to corresponding QuickStart Guide: http://docs.fortinet.com/

Default management IP address: 192.168.1.99

Login credentials: admin/<blank password>

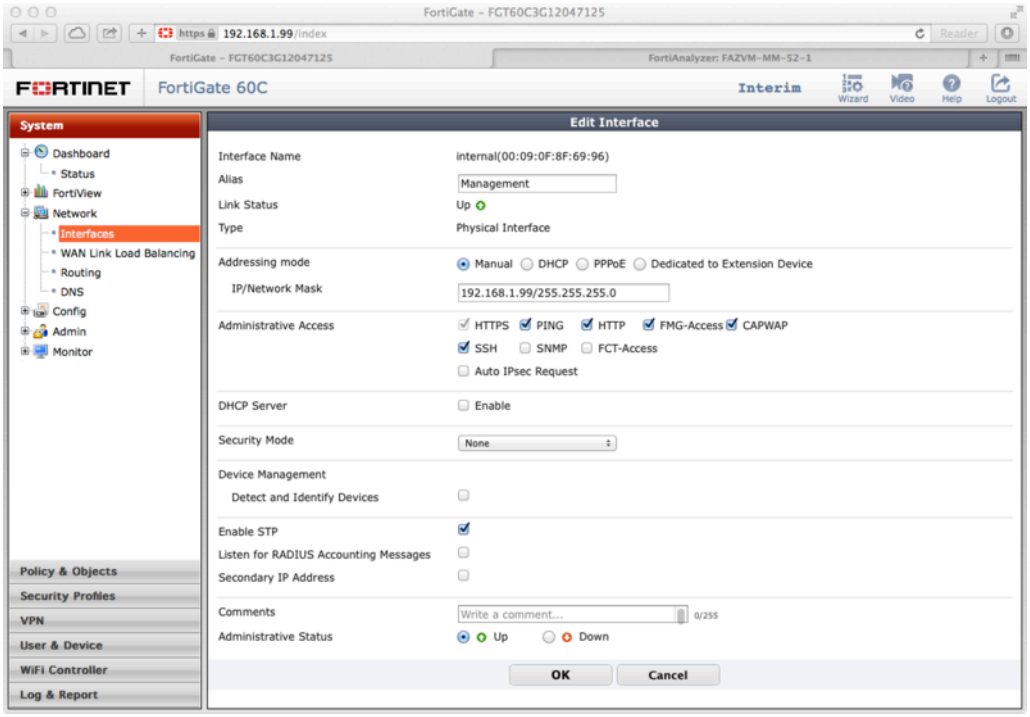
CLI

```
config system interface
    edit "internal"
        set vdom "root"
        set ip 192.168.1.99 255.255.255.0
        set allowaccess ping https ssh http fgfm capwap
        set type physical
        set alias "Management"
        set snmp-index 1
end
```

GUI

1. Go to System → Network → Interfaces
2. Select and Edit appropriate management interface.

3. Configure Alias as “Management” (optional)
4. Configure IP/Mask
5. Make sure DHCP checkmark is disabled
6. OK



Remember that your FortiGate must reach FortiGuard servers in order to do Web Filtering, update IPS/AV databases and engines.

Configure DNS Servers and routing in order to reach the Internet.

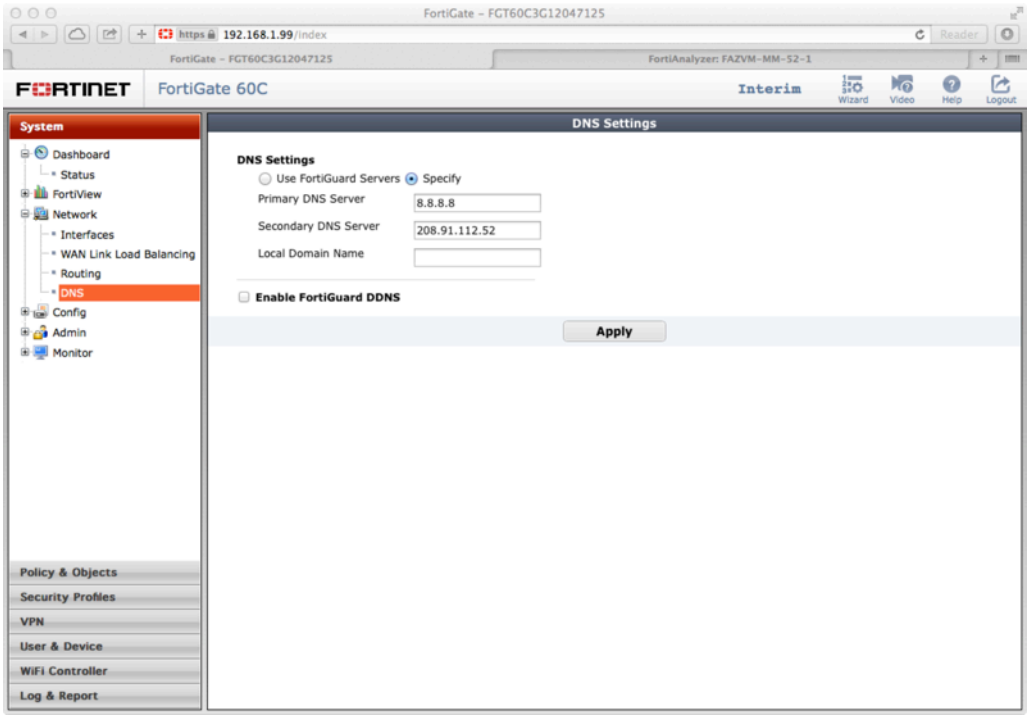
CONFIGURE DNS SERVERS:

CLI

```
config system dns
    set primary 8.8.8.8
    set secondary 208.91.112.52
end
```

GUI

1. Go to System → Network → DNS
2. Configure Primary and Secondary DNS
3. Apply



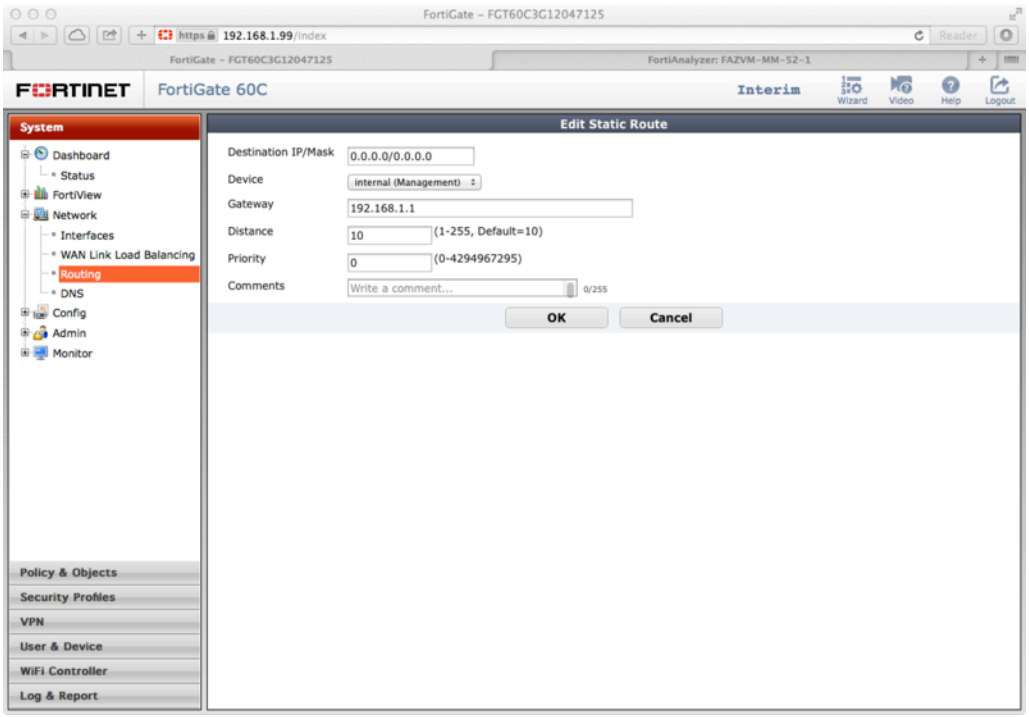
CONFIGURE DEFAULT GATEWAY

CLI

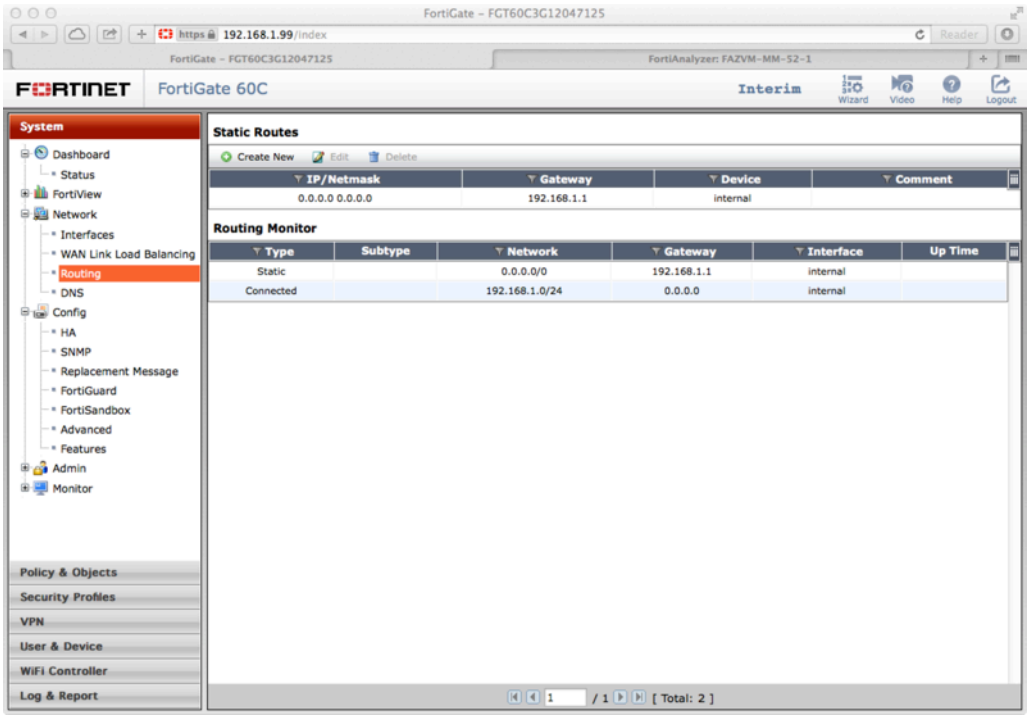
```
config router static
    edit 0
        set device "internal"
        set gateway 192.168.1.1
end
```

GUI

1. Go to System → Network → Routing
2. Under Static Routes: Create New



3. Add Gateway and outgoing Device (i.e. interface facing default gateway).
4. OK



VERIFY ROUTING TABLE

CLI

```
# get router info routing-table all
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter
area
       * - candidate default

S*      0.0.0.0/0 [10/0] via 192.168.1.1, internal
C       192.168.1.0/24 is directly connected, internal
```

Verify you are able to reach an Internet host:

CLI

```
FGT60C3G12047125 # exec ping www.fortinet.com
PING www.fortinet.com (66.171.121.34): 56 data bytes
64 bytes from 66.171.121.34: icmp_seq=0 ttl=45 time=245.6 ms
64 bytes from 66.171.121.34: icmp_seq=1 ttl=45 time=244.7 ms
```

```
64 bytes from 66.171.121.34: icmp_seq=2 ttl=45 time=243.8 ms
64 bytes from 66.171.121.34: icmp_seq=3 ttl=45 time=252.8 ms
64 bytes from 66.171.121.34: icmp_seq=4 ttl=45 time=244.0 ms

--- www.fortinet.com ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 243.8/246.1/252.8 ms
```

UPDATE YOUR SECURITY SERVICES DATABASES

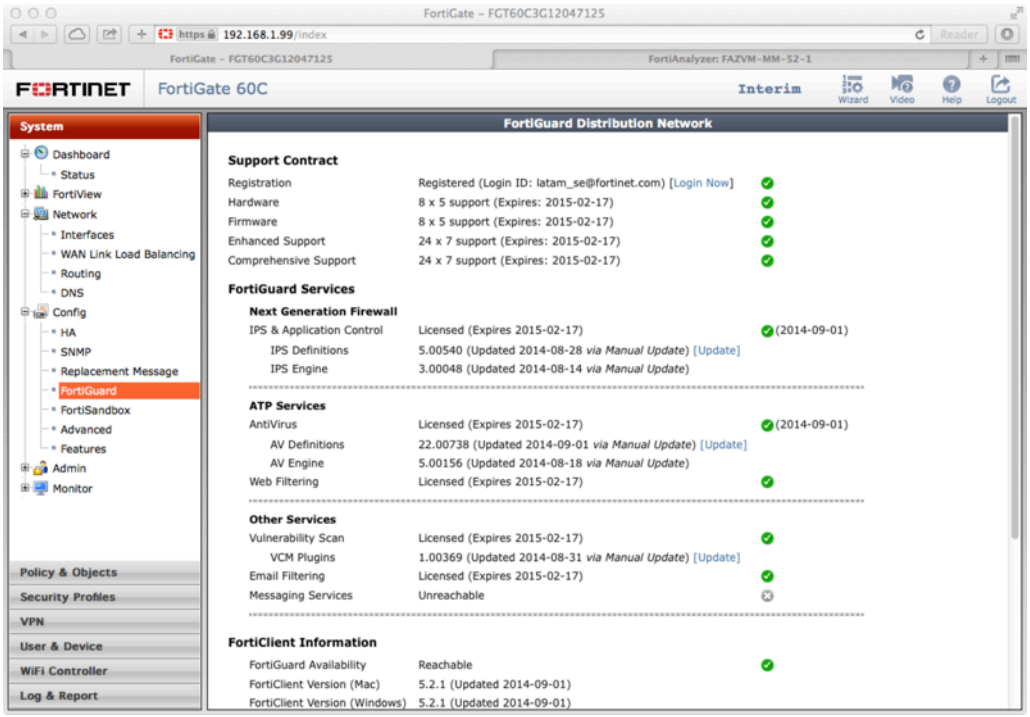
Once your unit has access to Internet is the right time to update your FortiGate's security services databases. Having up-to-date databases and engines is a key part of the Proof of Concept as this will improve catch-rates, performance and customer overall impression.

CLI

```
# exec update-now
```

GUI

1. Go to System → Config → FortiGuard
2. Expand the "AV & IPS Download Options" section and click on "Update Now"
3. Make sure FortiGuard Subscription Services appear with a green check mark at least for Antivirus, IPS & Application Control and Web Filtering



NOTE

By default, FortiGate uses port UDP/53 for communicating with the FortiGuard servers. It might be the case that a filtering device blocks this traffic for not being DNS (e.g. a DPI in the network). If that's the case, you have the option of using port UDP/8888

CONFIGURE TRAFFIC INTERFACE (SNIFFER)

Configure the interface that is going to be wired to the SPAN/Mirror port in the switch.

Remember to delete any reference (policies, routes, etc.) to the interface before changing it to sniffer-mode.

BEST PRACTICE TIP

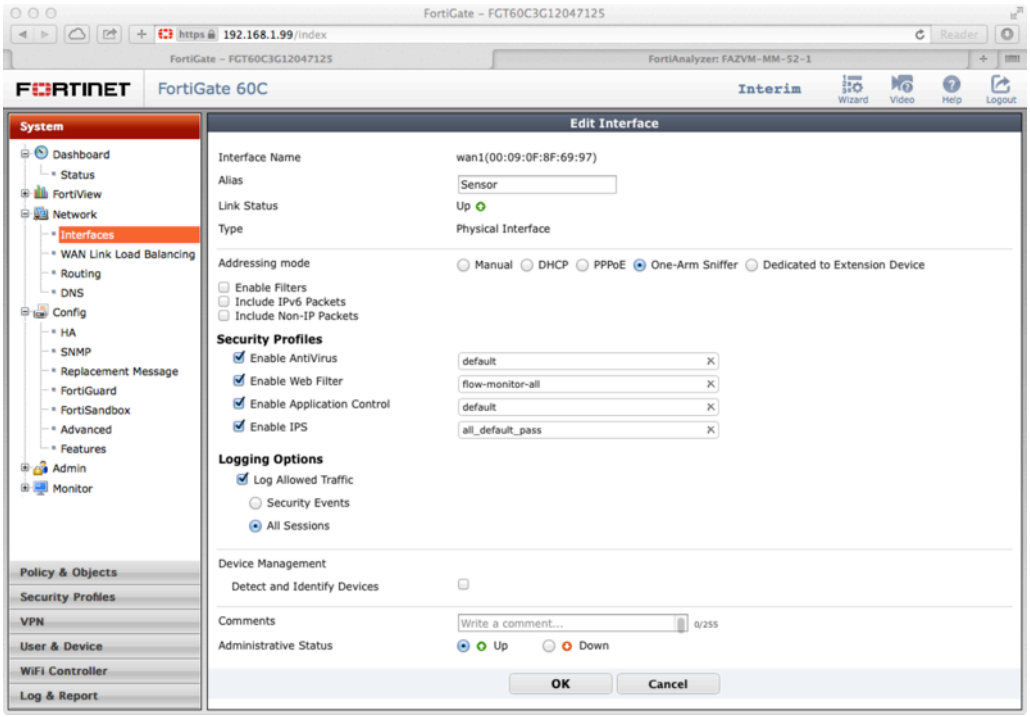
Using different interfaces for sniffing and management is recommended

CLI

```
config system interface
    edit "wan1"
        set vdom "root"
        set allowaccess ping
        set ips-sniffer-mode enable
        set type physical
        set alias "Sensor"
        set snmp-index 2
end
```

GUI

1. Go to System → Network → Interfaces
2. Select and Edit appropriate traffic interface.
3. Configure Alias as “Sensor” (optional)
4. Select “One-Arm Sniffer” as Addressing Mode
5. OK



CONFIGURE SECURITY PROFILES

In the next steps we will configure security profiles that will be used for traffic inspection. Be aware that when running in sniffer mode, only “flow-based” security profiles should be used, as there’s no possibility for proxies to intercept connections on this mode.

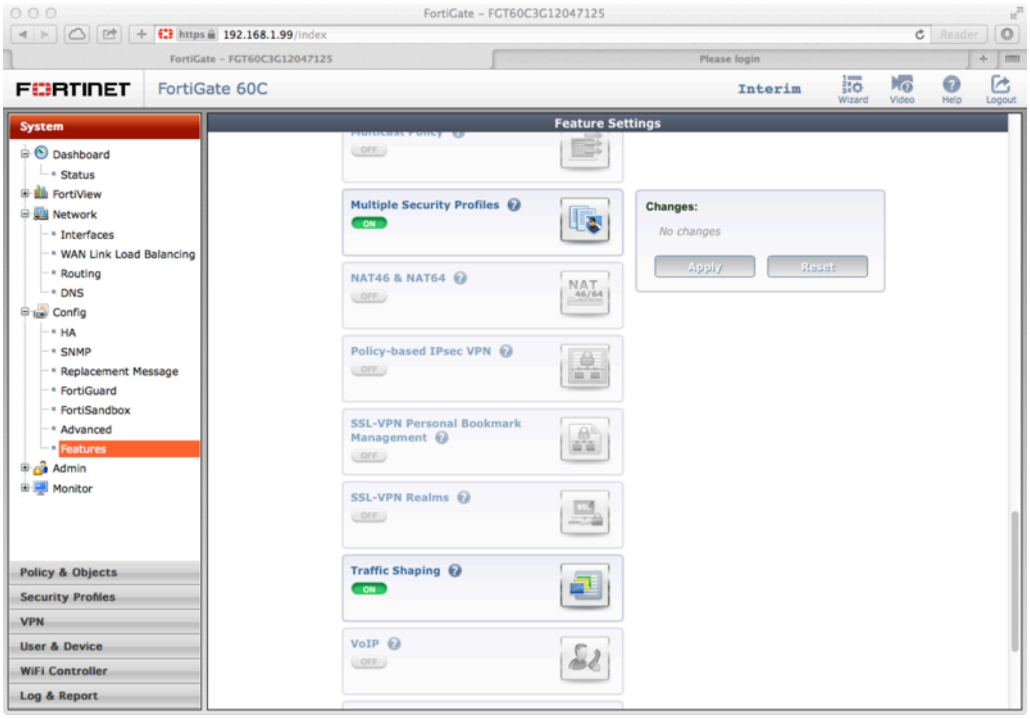
Enable multiple UTM profiles: If you’re using an entry level FortiGate you will probably have to enable the use of multiple UTM profiles, as by default just one profile per functionality can be configured. You might need to enable IPS for being shown in the GUI as well.

CLI

```
config system global
    set gui-ips enable
    set gui-multiple-utm-profiles enable
end
```

GUI

1. Go to System → Config → Features
2. Enable Intrusion Protection
3. Click on “Show More”
4. Enable Multiple Security Profiles
5. Apply



For the purpose of this document we will use FortiGate pre-configured profiles and highlight in bold letter any alteration you need to do from the default.

IMPORTANT

Some of the settings on this section cannot be done through the GUI. Once you finish your configuration check the profiles using CLI and make appropriate changes if necessary.

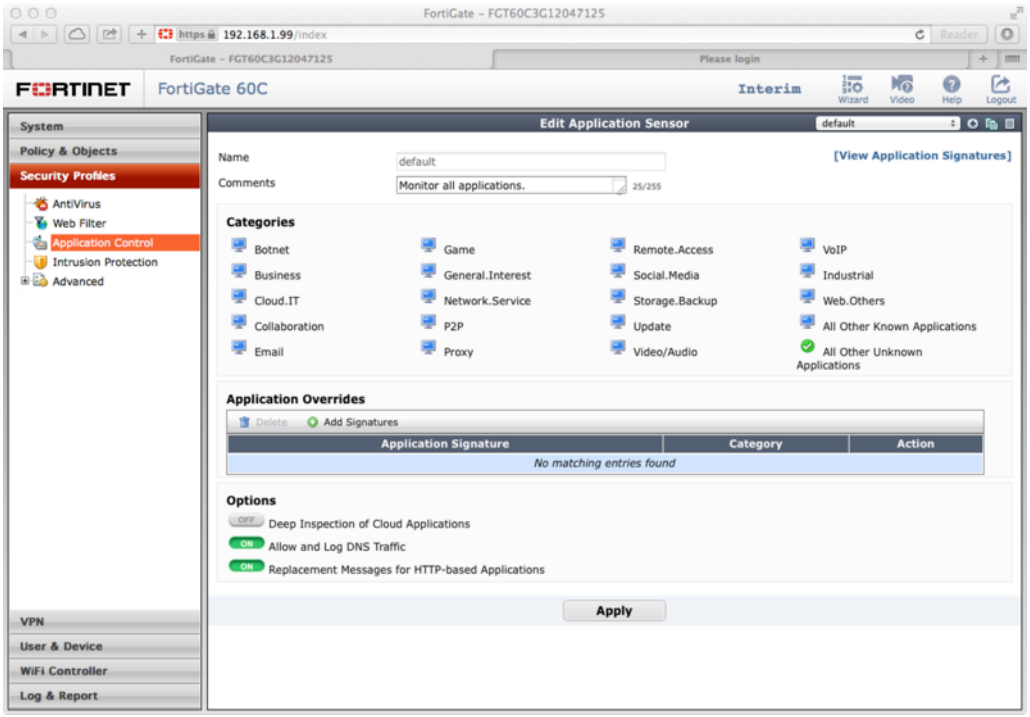
Configure Application Control sensor:

CLI ONLY

```
config application list
    edit "default"
        set comment "Monitor all applications."
        set other-application-log enable
            config entries
                edit 1
                    set action pass
                next
            end
    next
end
```

GUI

1. Go to Security Profiles → Application Control
2. Select “default” from the dropdown list menu
3. Apply



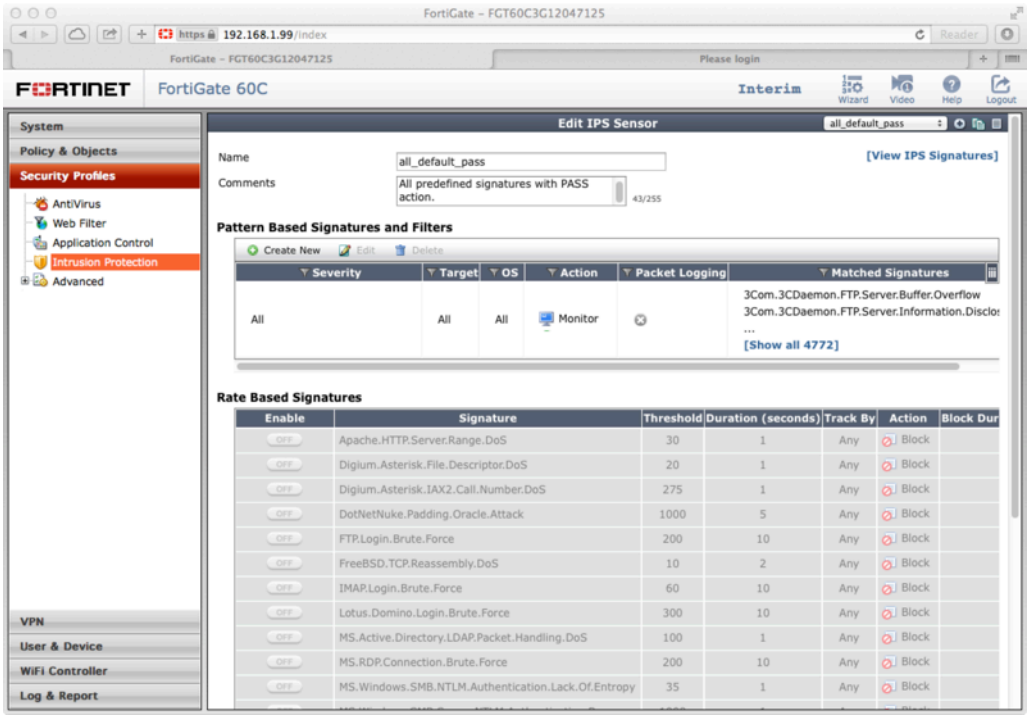
Configure IPS Sensor:

CLI

```
config ips sensor
    edit "all_default_pass"
        set comment "all predefined signatures with PASS action"
            config entries
                edit 1
                    set action pass
                    set status enable
                next
            end
    next
end
```

GUI

1. Go to Security Profiles → Intrusion Prevention
2. Select “all_default_pass” from the dropdown list menu
3. Apply



CONFIGURE SNIFFER POLICY

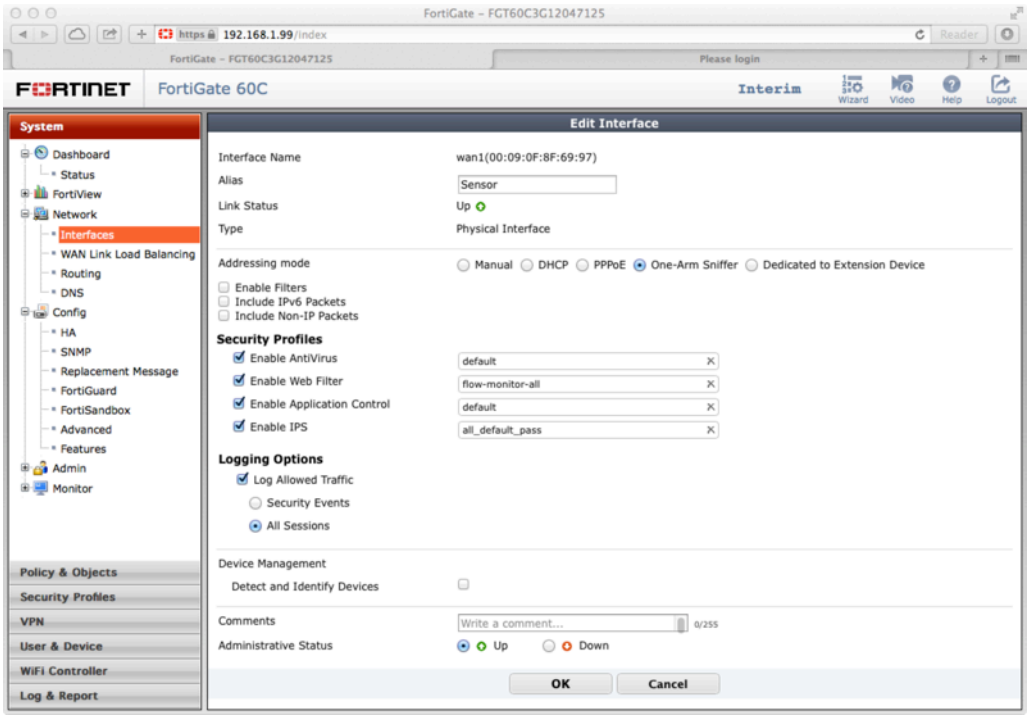
Once the basic networking has been configured and security profiles have been defined, we just need to put both things together. Creating a special kind of policies known as “sniffer policies” will do this.

CLI

```
config firewall sniffer
    edit 0
        set logtraffic all
        set interface "wan1"
        set application-list-status enable
        set application-list "default"
        set ips-sensor-status enable
        set ips-sensor "all_default_pass"
        set av-profile-status enable
        set av-profile "default"
        set webfilter-profile-status enable
        set webfilter-profile "flow-monitor-all"
end
```

GUI

1. Go to System → Network → Interfaces
2. Edit appropriate traffic interface.
3. Enable Security Profiles for Antivirus, Web Filter, Application Control and IPS, select recently configured profiles.
4. Select “Log Allowed Traffic” and “All Sessions”.
5. OK


FortiGate – FGT60C3G12047125
https 192.168.1.99/index
Reader
FortiGate – FGT60C3G12047125
Please login
FORTINET
FortiGate 60C
Interim
Wizard
Video
Help
Logout
System
Dashboard
Status
FortiView
Network
Interfaces
WAN Link Load Balancing
Routing
DNS
Config
HA
SNMP
Replacement Message
FortiGuard
FortiSandbox
Advanced
Features
Admin
Monitor
Policy & Objects
Security Profiles
VPN
User & Device
WiFi Controller
Log & Report
Edit Interface
Interface Name
wan1(00:09:0F:8F:69:97)
Alias
Sensor
Link Status
Up
Type
Physical Interface
Addressing mode
Manual
DHCP
PPPoE
One-Arm Sniffer
Dedicated to Extension Device
Enable Filters
Include IPv6 Packets
Include Non-IP Packets
Security Profiles
Enable AntiVirus
default
Enable Web Filter
flow-monitor-all
Enable Application Control
default
Enable IPS
all_default_pass
Logging Options
Log Allowed Traffic
Security Events
All Sessions
Device Management
Detect and Identify Devices
Comments
Write a comment...
0/255
Administrative Status
Up
Down
OK
Cancel

HANDS-ON: FORTIANALYZER CONFIGURATION

In order to provide better visibility and full reporting we will integrate the FortiGate device with a FortiAnalyzer. Let's remember FortiAnalyzer is the security architecture component that allows for a more professional reporting, compared to the basic reporting done by the FortiGate.

CONFIGURE FORTIGATE LOGGING TO FORTIANALYZER

CLI

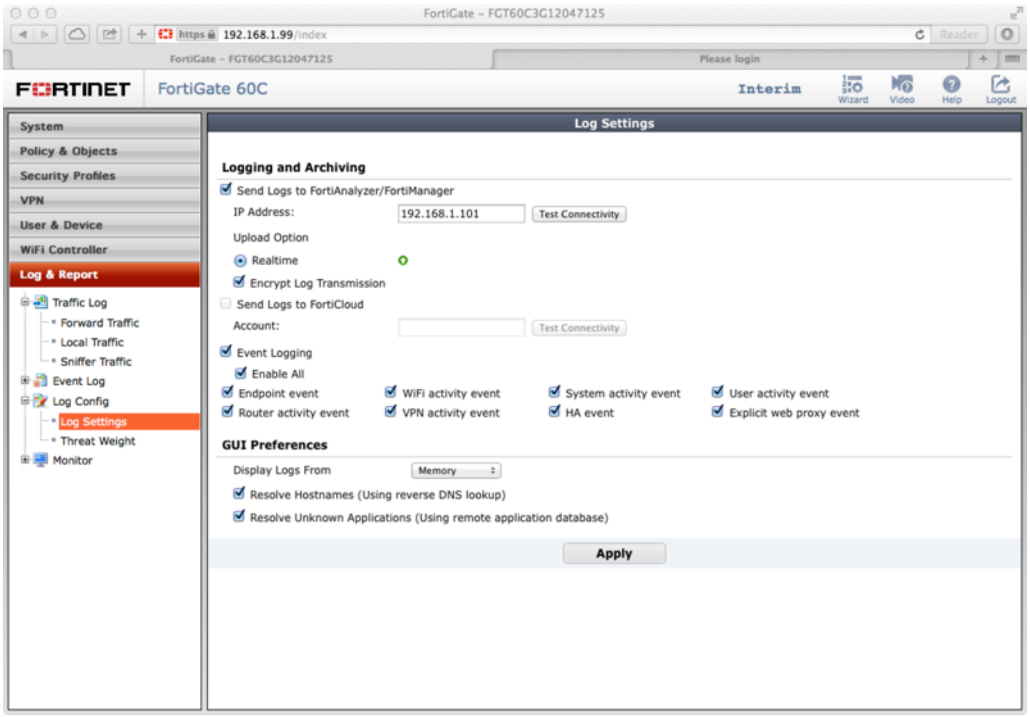
```
config log fortianalyzer setting
    set status enable
    set server 192.168.1.101
end
```

GUI

1. Go to Log & Report → Log Config → Log Settings
2. Enable "Send Logs to FortiAnalyzer/FortiManager"
3. Configure FortiAnalyzer's IP address
4. Apply

NOTE

When doing "Test Connectivity" you might get an error as the device hasn't been accepted in the FortiAnalyzer yet.

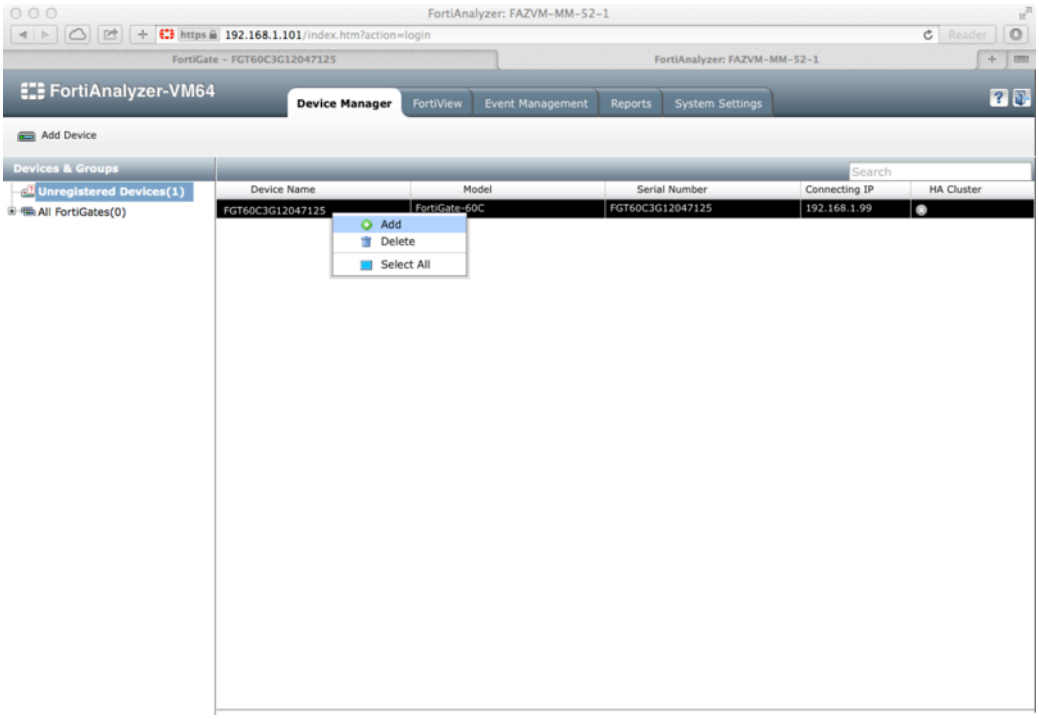


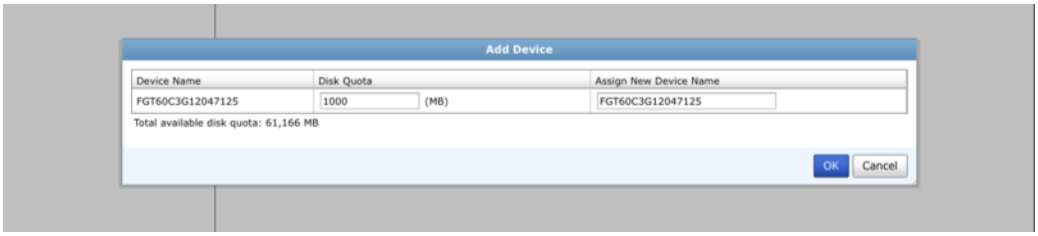
CONFIGURE FORTIANALIZER FOR ACCEPTING FORTIGATE LOGGING

After configuring the FortiGate to send logs to FortiAnalyzer, you will need to accept the devices as logging resource. This is done from FortiAnalyzer's GUI.

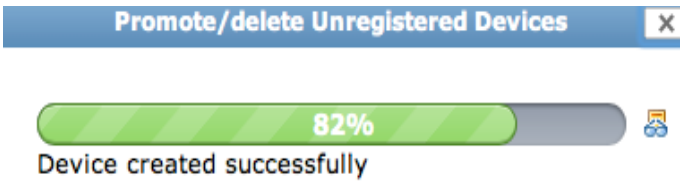
GUI

1. Login to FortiAnalyzer GUI using HTTP/S
2. Go to Device Manager tab
3. Look into "Unregistered Devices" list
4. Make sure you select the proper FortiGate in the list, right-click and select "Add" from the list.

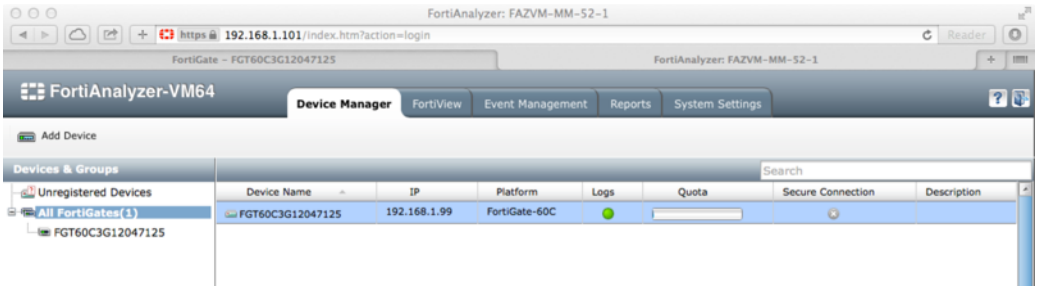




5. Set Disk Quota and Device Name
6. Click “OK” and wait until the process finish.



7. Verify your FortiGate appears listed as an accepted device.



BEST PRACTICE TIP

For POCs, make sure you modify FortiGate's quota and assign as much space as possible in the FortiAnalyzer. You don't want to start overwriting logs. Right click over the FGT → Edit → "Disk Log Quota" field

HANDS-ON: PUTTING ALL TOGETHER – NETWORK CONFIGURATION

Once FortiGate and FortiAnalyzer have been configured, the last step would be setting up the network in order to send traffic to the FortiGate.

CONFIGURE SWITCH

The FortiGate will receive traffic from a networking switch. First thing to understand is that because of this the FortiGate will only have visibility of traffic being redirected by this switch.

For the purpose of this Proof of Concept (POC) the recommendation would be to plug the FortiGate to the switch that receives all Internet traffic.

Configure SPAN/Mirror port:

This activity has to be done by company's networking specialists.

In order for FortiGate to get appropriate information, provides visibility and reporting, traffic in both directions should be copied/mirrored.

VERIFY CONFIGURATION

Once the switch has been configured everything is ready to start analyzing traffic. Before getting into graphics and reporting make sure you verify that FortiGate is actually receiving traffic. This can be done by running a TCP dump on sniffing configured interface:

CLI

```
# diagnose sniffer packet wan1 '' 1
interfaces=[wan1]
filters=[]
0.592415 200.42.92.139.1935 -> 192.168.1.44.53307: psh 2596606569
ack 2829680690
0.592770 192.168.1.44.53307 -> 200.42.92.139.1935: ack 2596606587
```

```
…
…
…

66 packets received by filter
0 packets dropped by kernel
```

HANS-ON: REVIEWING LOGS AND GENERATING REPORTS

Once your FortiGate and your networking device are configured you will be able to view logs, filter them and create reports. We will not go through the process of generating new reports but using predefined ones.

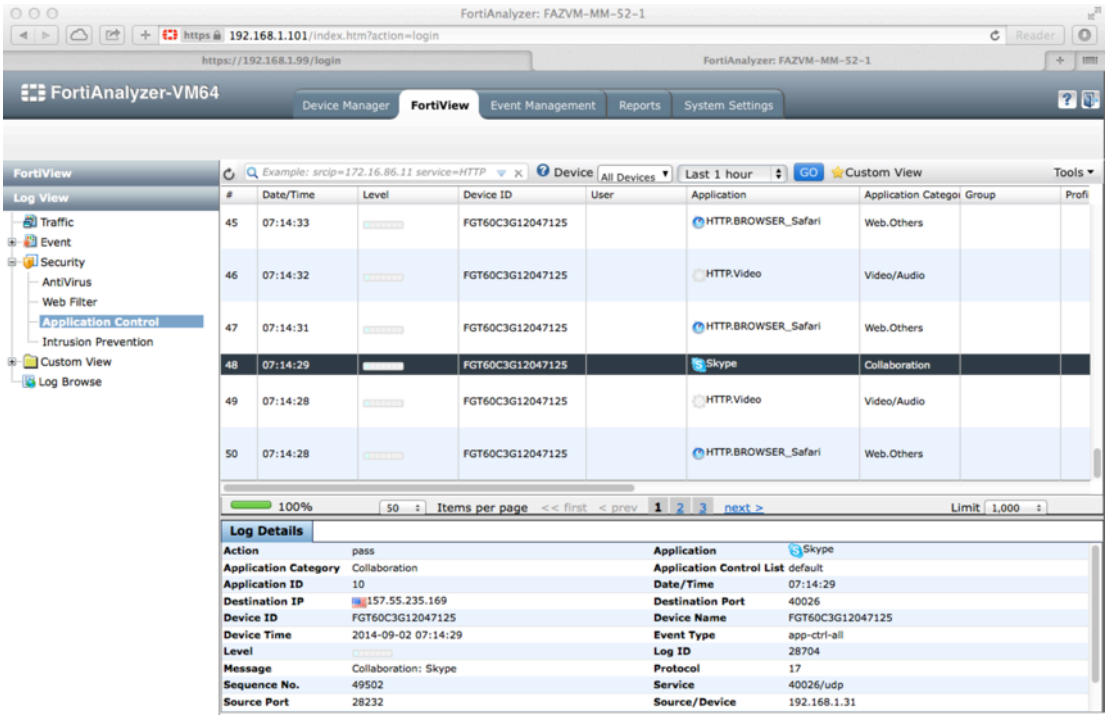
VIEWING LOS IN FORTIANALYZER

GUI

1. Login to FortiAnalyzer using HTTPS
2. Go to FortiView tab and select “Log View” from left menu.
3. On left pane, select Security → Application Control (other logs can be used for this example)
4. On right pane you should see a list of the log entries
5. Select any entry a see details below.

NOTE

If you can’t see log details, make sure “Display Log Details” is enable within the Tools menu



Filtering logs in FortiAnalyzer

GUI

There're two ways of using filters with FortiAnalyzer 5.2:

1. Using the top filtering bar

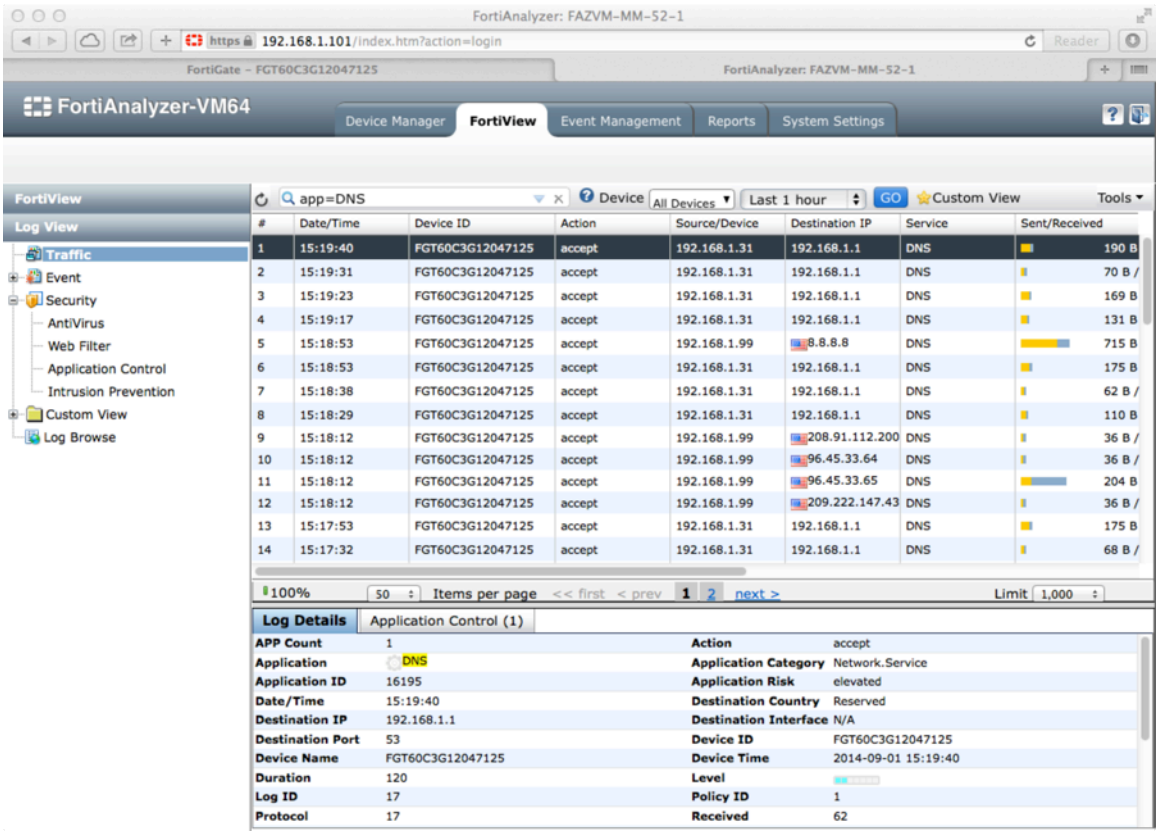
   Top filtering bar allows you to use free text in combination with some tags in order to search for records in an easy and fast way.

   Some example of searches you could do:

   - app=dns
   - app=youtu*
   - appcat=vide*
   - dstport=80 and srcip=192.168.1.*

NOTE

In order to ease your free text search, make sure you uncheck “Case Sensitive Search” using the Tools menu

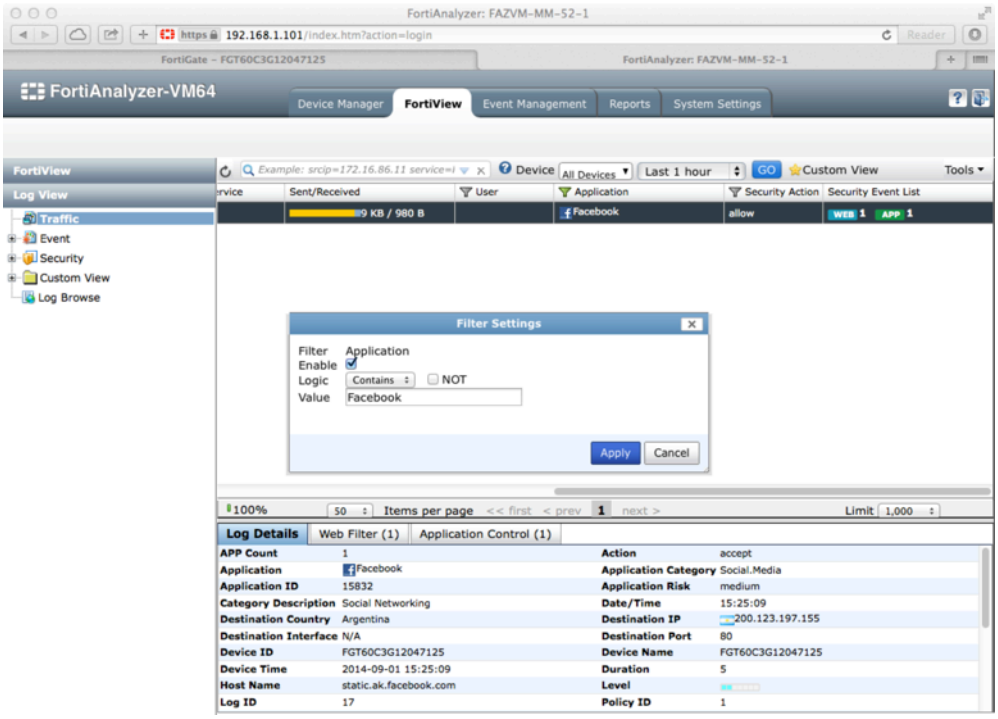


2. Using column filters

   Column filters are the traditional way of filtering records by specifying the desired value on each column. When filters in more than one column are specified they are joined by a logical AND, so all filters have to match in order for logs to appear.

NOTE

Column filters are not enabled by default. Click on Tools Menu and enable them.



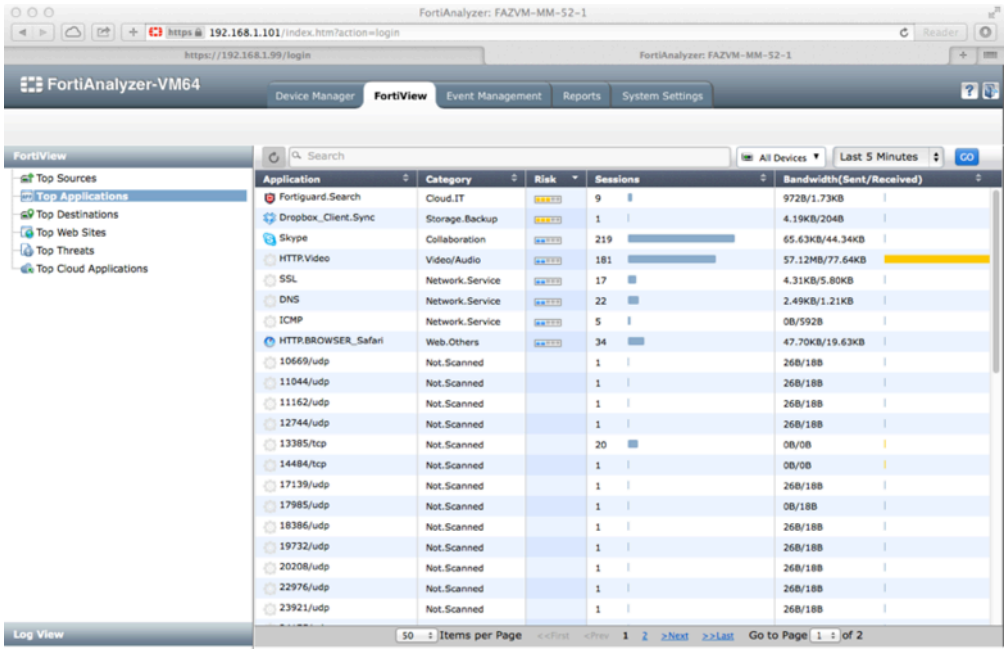
Click on the filter icon over the column to specify the desire value for it.

SHOWING REALTIME DATA WITH FORTIVIEW

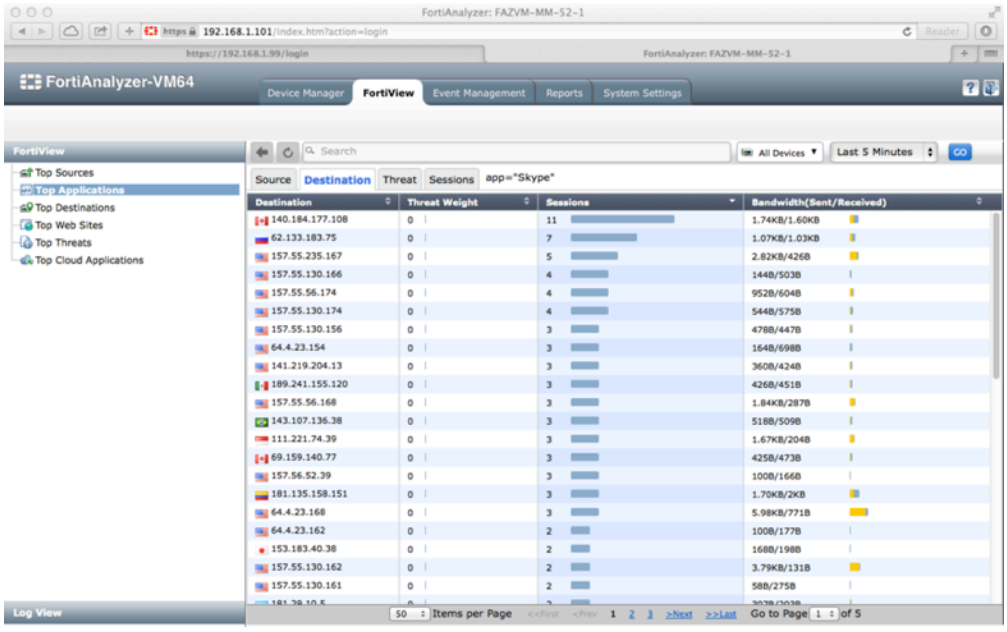
FortiView is the new functionality in FortiOS 5.2 that allows viewing real time information.

GUI

1. Go to FortiView tab
2. Click in any of the predefined views on the left pane. For instance “Top Applications”.
3. The right pane will show tables and graphs with real time information.



4. Note that you can drill down until you find the level of detail you want.

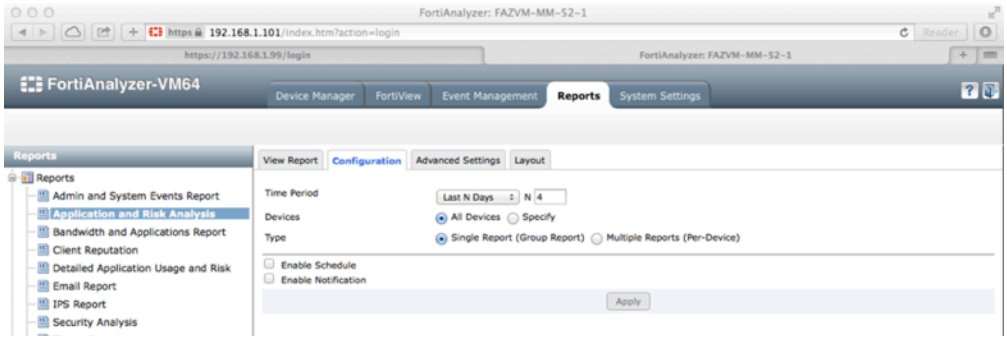


GENERATING REPORTS IN FORTIANALYZER

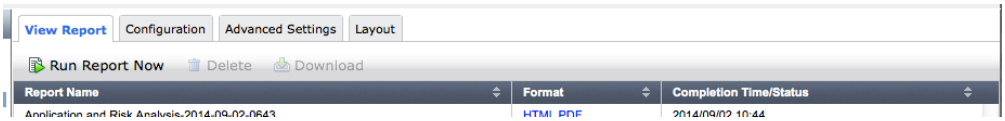
This section will show how to use and generate pre-configured reports. Generating new reports is outside the scope of this document.

GUI

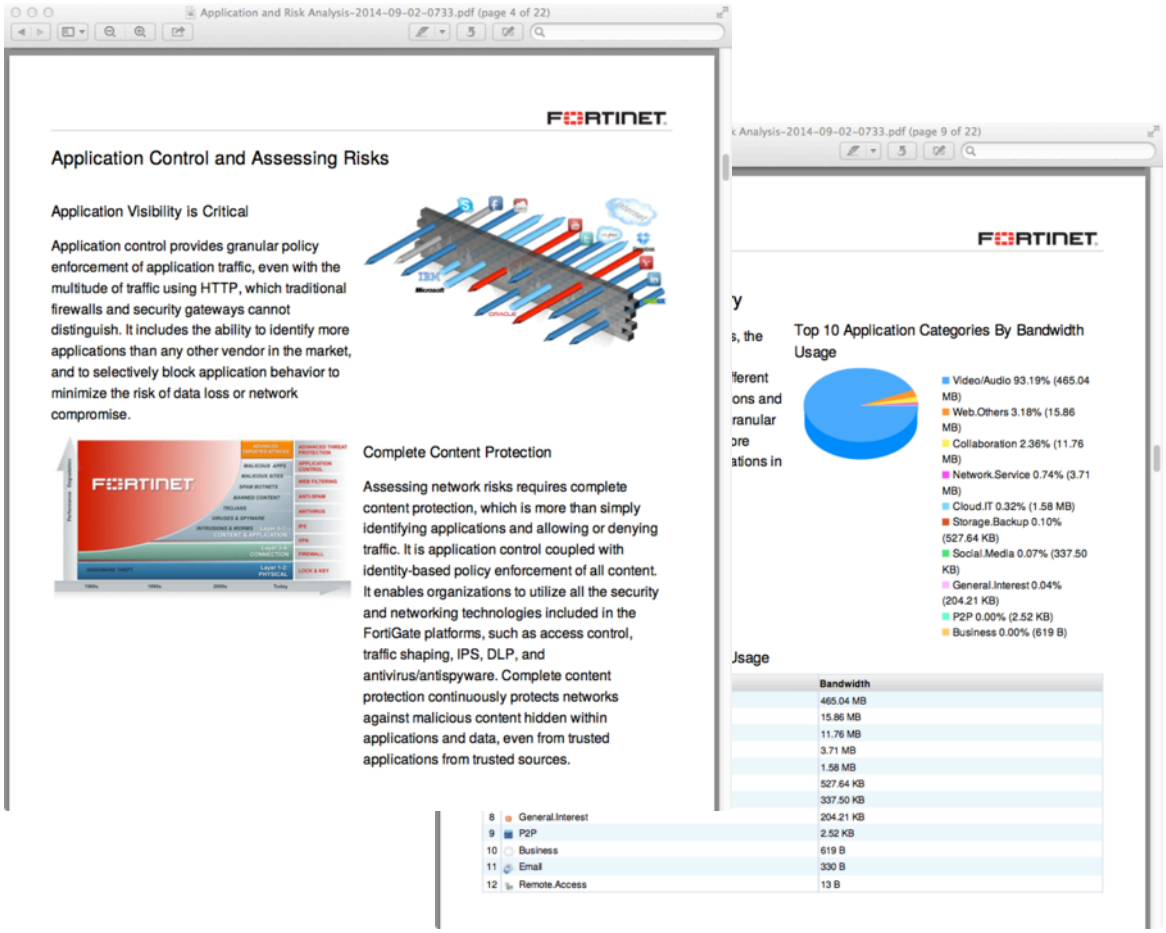
5. Go to Reports tab
6. Click in any of the predefined reports on the left reports tree.
7. Within the “Configuration” make sure you select the “Time Period” of your choice according to the time the device has been collecting logs. Also make sure “All Devices” is selected in the Devices option.



8. Click Apply
9. Go to the “View Report” tab and then “Run Report Now”



10. Wait until the report has been generated and click either on PDF or HTML in order to view it in your preferred format.
11. Analyze the generated report



Even though you can benefit from many of the predefined reports, it is recommended at least generate the followings for the POC:

- **Admin and System Events Report**: Get auditing information administrative events done in the platform.
- **Application and Risk Analysis**: Risk based analysis of security events.
- **User Report**: Per user comprehensive analysis

REPORT PRESENTATION TIPS

1. Review and familiarize with each report. In case there're blank sections, make sure you are prepared to answer why.
2. Do not email the reports to your customer. You will cause a very positive impact if you print it and share it with your customer face to face. Keep in mind the report is very valuable and will often reveal new information about the customer's network.
3. Do your homework. Look through the report and determine problematic areas (threats, bandwidth, etc.). Be prepared to make recommendations about applications, web and bandwidth usage.
4. Use FortiGuard (http://www.fortiguard.com) to research any anomalies that arise prior to your visit.

APPENDIX I – ACTIVE DIRECTORY INTEGRATION (USER IDENTIFICATION AND REPORTING)

For many years FortiOS has had the ability of defining and enforcing user/group based policies. In the case of one-arm deployments is possible to leverage this capability to identify users for logging and reporting.

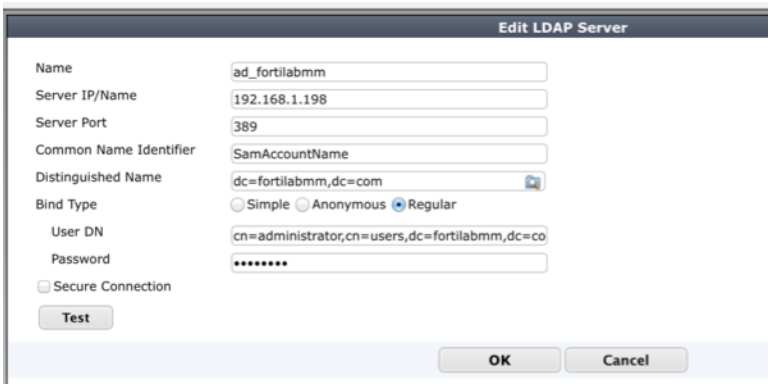
This appendix's goal is showing how to do a basic configuration for Microsoft Active Directory integration by means of Single Sign-On functionality, built-in in FortiOS. Is important noting that the configuration shown here might not be suitable for all cases. Depending on the complexity of the Active Directory deployment more advanced configurations could be required (e.g. FSSO deployment, multiple collectors, etc.). Please review FortiOS 5.2 Handbook Authentication for FortiOS 5.2 for more information.

ADDING AN LDAP SERVER

The first step is to configure and LDAP Server in order to read objects such as users and groups from Active Directory's database.

GUI

1. Go to User & Device → Authentication → LDAP Servers
2. Click on Create New
3. Fill the information according to LDAP configuration



4. Make sure the connection test is successful

NOTE

When integrating with Active Directory consider that:

- Common Name Identifier must be “sAMAccountName”
- Bind Type must be “Regular”
- User DN: Make sure you fill with complete DN. You cannot use just the username.

CLI

```
config user ldap
    edit "ad_fortilabmm"
        set server "192.168.1.198"
        set cnid "SamAccountName"
        set dn "dc=fortilabmm,dc=com"
        set type regular
        set username
"cn=administrator,cn=users,dc=fortilabmm,dc=com"
        set password 123456
end
```

ADDING A SINGLE SIGN-ON SERVER

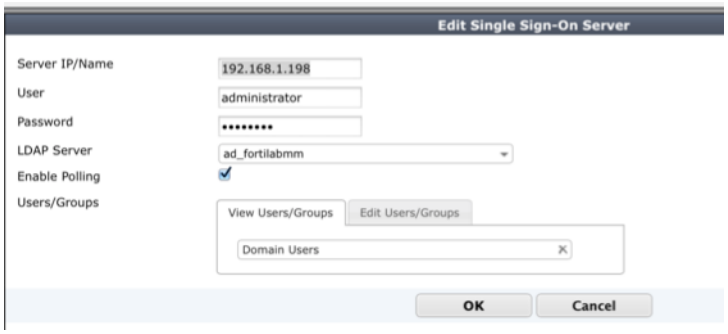
The Single Sign-On configuration will indicate the FortiGate how to poll Active Directory’s database in order to get user, group and session information.

GUI

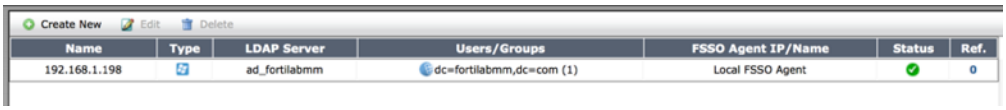
1. Go to User & Device → Authentication → Single Sign-On
2. Click on Create New
3. Fill the information according to Active Directory’s Global Catalog server configuration
4. Click on “Edit Users/Groups” and make sure you select the group or groups of users you want to monitor.

NOTE

In case you want to collect information from all users, something expected in a POC, you can simplify the configuration by selecting one group for which all users are members (e.g. “Domain Users”).



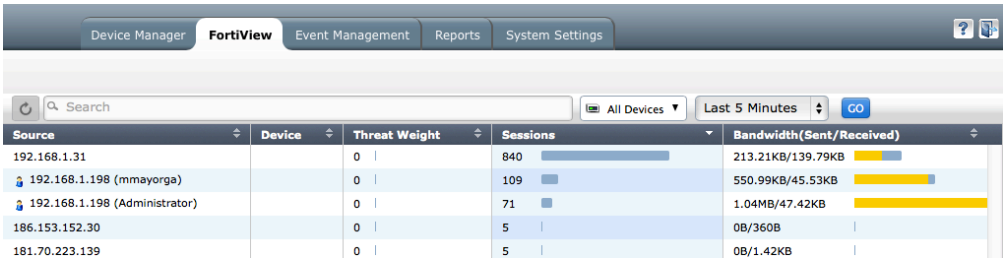
5. Selected groups must appear under “View Users/Groups”
6. Click OK
7. Make sure you have a green checkmark under Status

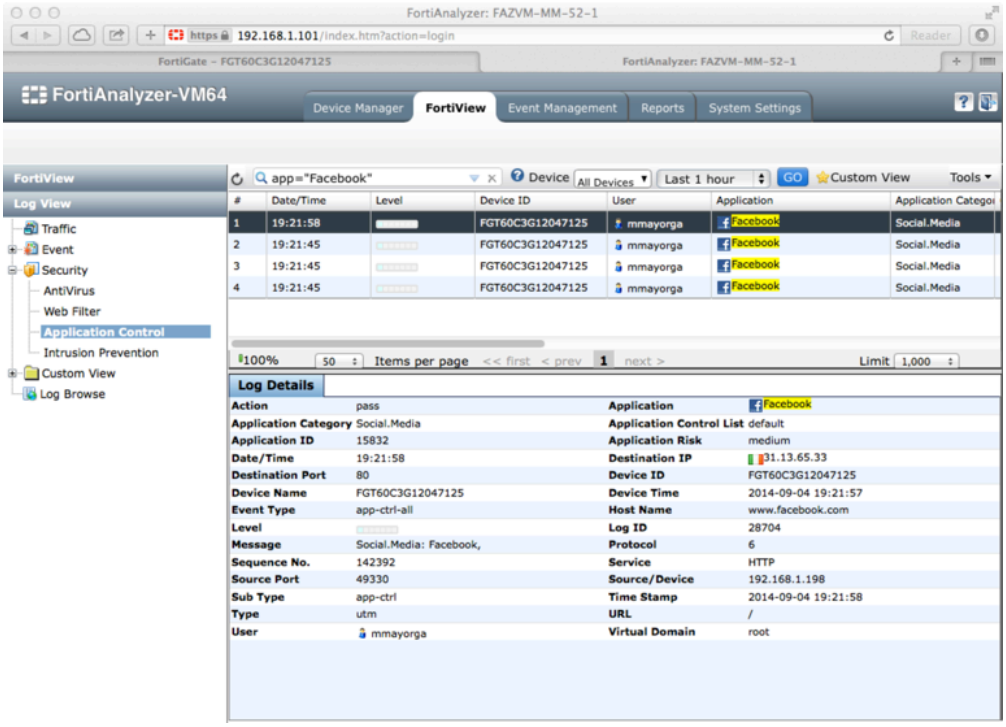


CLI

```
config user fsso-polling
    edit 0
        set server "192.168.1.198"
        set user "administrator"
        set password 123456
        set ldap-server "ad_fortilabmm"
            config adgrp
                edit "CN=Domain
Users,CN=Users,dc=fortilabmm,dc=com"
                next
            end
    next
end
```

You can now access your FortiAnalyzer and check that is showing usernames in FortiView, Log View and Reports.





APPENDIX II – SNIFFER MODE – POC CHECK LIST

STEP ZERO

- ☐ Do all this procedure on a controlled network (your own company network for instance) at least once before attempting it on a customer.

BEFORE DOING ANY CONFIGURATION

- ☐ Call the customer. Gather all information you will need during the POC.
- ☐ Make sure products are registered, with valid FortiGuard contracts and proper FortiOS versions.
- ☐ Make sure paperwork has been done and that you won't have any logistic issue to get the equipment inserted into customer's network.

CONFIGURING FORTIGATE

- ☐ Do a factory reset.
- ☐ Configure networking: Management interface, DNS, default gateway and other routes. Test your networking configuration.
- ☐ Update FortiGuard signatures and engines.
- ☐ Configure sniffing interface.
- ☐ Configure security profiles: Application Control and IPS (you can use defaults for others).
- ☐ Configure sniffing policy.

CONFIGURING FORTIANALYZER

- ☐ Setup FortiAnalyzer.
- ☐ Configure FortiGate to send logs to FortiAnalyzer.

- Setup networking (switch, router) so traffic gets copied to FortiGate.
- Verify that the FortiGate is receiving network traffic.
- Review logs, FortiView and generate reports.
- Setup a meeting and present reports to the customer.
- Make sure you send a follow-up email with a report summarizing the results of the POC.
- Sell!

APPENDIX III – QUICK CONFIGURATION SCRIPT

```
# POC Sniffer Mode
# Quick Configuration Script

# Please change variables below accordingly to your environment
# and then replace all instances of the strings throughout the
# script
#
# <mgmt_interface>
# <mgmt_ip>
# <mgmt_netmask>
# <mgmt_gateway>
# <sniffer_interface>
# <faz_ip>
#


# Factory reset at the beginning
exec factoryreset
y
# Wait the reboot

# Disable DHCP Server
config system dhcp server
    purge
    y
end

# Configure management interface
config system interface
    edit "<mgmt_interface>"
        set vdom "root"
        set ip <mgmt_ip> <mgmt_netmask>
        set allowaccess ping https ssh http fgfm capwap
        set type physical
        set alias "Management"
        set snmp-index 1
    next
end

# Configure DNS servers
config system dns
    set primary 8.8.8.8
    set secondary 208.91.112.52
end

# Configure default gateway
config router static
      edit 0
          set device "<mgmt_interface>"
          set gateway <mgmt_gateway>
      next
```

```
end

# Check your Internet connection and name resolution
exec ping www.yahoo.com

# Update FortiGuard services (AV, IPS, AppCtrl, etc.)
exec update-now

# Check if FortiGuard version are updated
get system status

# Configure sniffer interface
config system interface
    edit "<sniffer_interface>"
        set vdom "root"
        set allowaccess ping
        set ips-sniffer-mode enable
        set type physical
        set alias "Sensor"
        set snmp-index 2
    next
end

# Configure enable IPS in the GUI and multiple security profiles
config system global
    set gui-ips enable
    set gui-multiple-utm-profiles enable
end

# Configure Application Control sensor
config application list
    edit "default"
        set comment "Monitor all applications."
        set other-application-log enable
            config entries
                edit 1
                    set action pass
                next
            end
    next
end

# Configure IPS sensor
config ips sensor
    edit "all_default_pass"
            config entries
                edit 1
                    set status enable
                    set action pass
                next
            end
    next
end
```

```
# Configure sniffer policy
config firewall sniffer
    edit 0
        set logtraffic all
        set interface "wan1"
        set application-list-status enable
        set application-list "default"
        set ips-sensor-status enable
        set ips-sensor "all_default_pass"
        set av-profile-status enable
        set av-profile "default"
        set webfilter-profile-status enable
        set webfilter-profile "flow-monitor-all"
    next
end
end

# Configure logging to FortiAnalyzer
config log fortianalyzer setting
    set status enable
    set server <faz_ip>
    set reliable enable
end

# Check that sniffer interface is receiving traffic
diagnose sniffer packet <sniffer_interface> '' 1
```

APPENDIX IV – REFERENCES

- CLI Reference Guide for FortiOS 5.2
  http://docs.fortinet.com/uploaded/files/1981/fortigate-cli-52.pdf

- Install and System Administration for FortiOS 5.2
  http://docs.fortinet.com/uploaded/files/2002/fortigate-system-admin-52.pdf

- FortiOS Handbook Authentication for FortiOS 5.2
  http://docs.fortinet.com/uploaded/files/1937/fortigate-authentication-52.pdf

- The FortiOS Cookbook 5.2
  http://docs.fortinet.com/uploaded/files/2021/fortigate-cookbook-52.pdf

- FortiAnalyzer v5.0 Administration Guide
  http://docs.fortinet.com/fa/50/FortiAnalyzer-504-Admin-Guide.pdf

- FortiGuard Center
  http://www.fortiguard.com